State of Arizona

Department of Economic Security Information Technology Standards	Title: 1-38-0064 DES Removable Media Policy	
Subject: This policy defines the use of removable media in the DES environment.	***Effective Date:*** 09/20/05	***Revision:*** 0

1. **Summary of Policy Changes**
   Original Implementation

2. **Purpose**
   This policy establishes guidelines and responsibilities regarding the use of removable media in the DES computing environment.

3. **Scope**
   This standard applies to all DES administrative entities, councils, divisions, administrations, programs and business partners.

4. **Responsibilities**
   4.1. The DES Director, Deputy Directors, and Assistant Directors are responsible for implementing and enforcing this policy.
   4.2. The DES CIO and the Division of Technology Services are responsible for implementing this policy.
   4.3. The DES Director, Deputy Directors, and Assistant Directors are responsible for identifying what constitutes as confidential and privileged data for their respective areas and how this type of data will be managed in relation to these devices.
   4.4. DES employees and business partners have the responsibility to take measures to ensure that DES data and systems remain protected.

5. **Definitions and Abbreviations**

   5.1 Definitions

   5.1.1. **Confidential Data/Information** – Any applicant, claimant, recipient, employer, employee or client data. Social Security numbers, names, addresses. This information is not generally available to the public.

   5.1.2 **Data Encryption Standard** – (DES) - is a standard cryptographic algorithm developed by the U.S. National Institute of Standards and Technology (NIST).

   5.1.3 **Encryption** - is the conversion of data into a form (cipher text) that cannot be easily read by unauthorized people.

   5.1.4 IT Equipment includes: **P**ersonal **C**omputers (PC), including desktops, and laptops.

5.1.5 **Protected Health Information (PHI):** Any health-related information that can be tied to an individual is considered protected health information.

5.1.6 **Public Information:** data that is made generally available without specific custodian approval and that has not been explicitly and authoritatively classified as confidential.

5.1.7 **Removable Media:** is any data storage unit that can be removed from the personal computer and taken with you. Drives to read removable media can either be installed internally into the computer itself or come as external units that must be plugged into the computer. There are all sorts of types of removable media. The most common types are:

5.1.8 **Floppy disc:** A typical high density floppy could hold 1.2 Mb of information after it was formatted. Due to the rapid increase of computer memory amounts floppy discs are becoming obsolete. There are several variations on the floppy disc with more modern memory capabilities these include the Zip (100-250 Mb), the Jaz (.5Gb-2Gb), and numerous other discs made by many manufacturers.

5.1.9 **Flash Cards:** CompactFlash, Secure Digital, Smart Media, Memory Stick, Jump Drive are the new generation of storage media. These cards are small but can store up to several gigabytes of data. (Some other types of these devices are called thumb drives and pen drives.)

5.1.10 **Tape Drives:** There are numerous types of tape drives for computer. Even DAT tape (typically used for audio) can be used for immense amounts (approximately 100 Gigabytes) of data storage.

5.1.11 C**D (Compact Disc):** For Data storage purposes a compact disc can hold 650 Mb or 700 Mb.

5.1.12 **CD writers:** are another type of drive. Typical CD's (CDRs) are a write once format. CD Rewritable (CDRW) is a multiple write format. There are also high definition CD's (HDCD) (24 bit recording instead of 16 bit recording). HDCD's need an HDCD player.

5.1.13 **DVD (Digital Versatile Disc):** DVD's are similar to CD's in look. They hold immense amounts of information (5-9 gigs). The amount varies due to various and developing types of compression. DVD RAM is a rewritable variation. Apple Superdrive is a CD/DVD writer player.

5.1.14 User – As used in this policy, User refers to a DES employee, contract employee, or other DES-authorized person who exchange electronic communications with DES.

5.2. Abbreviations

5.2.1 **CD** – **C**ompact **D**isc

5.2.2 **CIO** – **C**hief **I**nformation **O**fficer

5.2.3 **CISO** – **C**hief **I**nformation **S**ecurity **O**fficer

5.2.4 **DES** – **D**epartment of **E**conomic **S**ecurity

5.2.5 **DTS** – **D**ivision of **T**echnology **S**ervices

5.2.6 **DVD** – **D**igital **V**ideo **Disc** or **D**igital **V**ersatile **D**isc

5.2.7 **GITA** – **G**overnment **I**nformation **T**echnology Agency

5.2.8 **IT** – **I**nformation **T**echnology

5.2.9 **PC** – **P**ersonal **C**omputer

5.2.10 **PHI** – Protected Health Information

6. POLICY

Background Information about Removable media:

As with other technology, removable media technology is advancing at a rapid rate. Within the last decade we have gone from being able to store a minimal amount of data on a floppy disc to being able to store gigabytes of data on other types of removable devices. With the increased amount of storage capacity, the risks created by making DES data portable also increase.

- DES is obligated by state and federal laws to protect confidential data.
- Examples of confidential data are (but not limited to) client or employee-specific information that identifies an individual such as name, address, or Social Security Number and PHI (Protected Health Information).
- The potential of transmission of viruses and other malicious code increases when storage devices are moved from computer to computer to transfer data.
- With the increased amount of storage space available on these drives, the opportunity for pirating software and committing copyright infringement increases.
- Driver software (software required by some devices in order for the device to work with the computer) come with license agreements that need to be observed. Some drivers prohibit installation on multiple computers.
- Like other portable computing devices (PDA's and laptops), the risk for loss or theft is high.

6.1. Only DES-owned removable media/devices shall be connected to the DES network.

6.2. The Deputy and Assistant Directors for each division are responsible for identifying what data in their areas is public and what data is confidential.

6.3. Confidential data is not to be stored on removable media, unless encrypted or password protected.

6.4. Exceptions must be approved by the Deputy or Assistant Director for the Division and ISA must be notified of exceptions granted.

6.5. Virus protection software will be configured according to DES Virus and Malicious Code Policy to ensure that all drives and files are scanned prior to access.

6.6. When possible, removable media will be secure, using encryption or requiring passwords for accessing the devices, to minimize the impact if the device is lost or stolen.

6.7. If the removable media is not capable being secured (as defined in 7.6), then files containing confidential data stored on these removable devices shall use encryption and/or be password protected.

6.8. All reasonable measures shall be taken to prevent the loss or theft of removable media or other mass storage mobile devices.

7. **Implications**

7.1. This policy replaces all previous DES policy on the topics of removable media and supports agency policies referencing the management of DES assets, privileged and confidential information.

8. Implementation Strategy

8.1. This policy is effective immediately.

9. **References**

9.1. 1-38-0006 DES Information Security Policy

9.2. 1-38-0013 DES Virus and Malicious Code Policy

9.3. 1-38-0017 DES Client and Employee Information Transmission Policy

9.4. 1-38-0029 Information Technology (IT) and Office Equipment Resources Acceptable Use Policy

9.5. 1-38-0075 DES Physical Security Policy

9.6. Basic Data Security Training Manual

10. Attachments

10.1. None

11. Associated GITA IT Standards and Policies

11.1. P100 – Information Technology

11.2. P252 Rev. 1.0 – Intellectual Property Policy

11.3. P740 – S741 – Classification and Categorization of Data

11.4. P740 – S740 – Data Modeling

11.5. P800 – S860 Rev. 2.0 – Virus and Malicious Code Protection

11.6. P800 – S880 Rev 1.0 – Media Sanitization/Disposal

12. Review Date

12.1. This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.